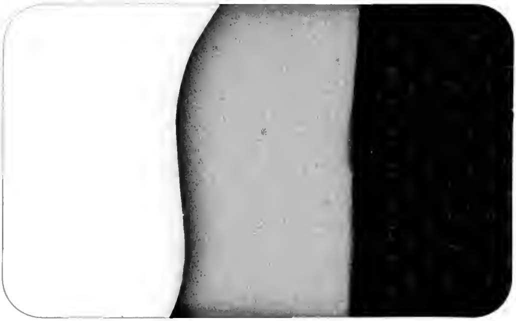
Isomorphism of Strongly Regular Graphs

by

Richard Cole

Technical Report No. 63

March 1983



Isomorphism of Strongly Regular Graphs

by

Richard Cole

Technical Report No. 63

March 1983

Abstract

We present isomorphism algorithms for k-strongly regular graphs running faster the larger k. A consequence of our proof is that no "interesting" graph is (d log n)-transitive, for some constant d.

1. Introduction

Attempts at general graph isomorphism algorithms often face difficulties with strongly regular graphs; for example, Corneil and Gotlieb [3], and Aspvall [1]. Corneil and Gotlieb parameterize the strongly regular graphs as k-strongly regular, k taking integer values. The larger k, the worse their proposed algorithm performs. We obtain isomorphism algorithms for k-strongly regular graphs running faster, the larger k. This work is of interest too because, by contrast with recent developments in graph isomorphism using group theoretic techniques [5,6,7], we use very simple methods.

We show there is an isomorphism algorithm for k-strongly regular graphs running in time $O(n^{cn^{1/k}}\log n)$ for some constant c, independent of k and n. In particular, for k=logn, this is a running time of $O(n^{\log n})$. Babai [2] gave an isomorphism algorithm for strongly regular graphs running in time $O(n^{n^{1/2}\log n})$, for some constant c. However, he did not consider k-strongly regular graphs. In [8] some isomorphism algorithms for restricted classes of strongly regular graphs are presented; they run in time $O(n^{c\log n})$, for some constant c.

In section 2 we give an outline of the algorithm and introduce the concept of a distinguishing set. In section 3 we outline the proof of the running time; details are given in the appendix. And in section 4 we discuss the significance of this work and possible further work.

2. The algorithm

Definition 1: Let G be a regular graph of degree $d_\emptyset$, and let $A(v_1,v_2,\ldots,v_r)$ be the set of vertices adjacent to all of $v_1,v_2,\ldots,v_r$.

G is <u>strongly regular</u> if there exist constants d_1, d_2 such that

(1) $|A(u,v)| = d_1$, if u and v are adjacent, and

(2) $|A(u,v)| = d_2$, if u and v are non-adjacent.

We also say these graphs are <u>2-strongly regular</u>. The definition of a k-strongly regular graph is similar: we require, for all $h \leq k$, that $|A(v_1, v_2, \ldots, v_h)|$ be dependent solely on the isomorphism type of the subgraph of G induced by the vertices $v_1, v_2, \ldots, v_h$. Clearly, a (k+1)-strongly regular graph is k-strongly regular.

<u>Definition 2</u>: Let G be a graph. We say G is 2-transitive if each edge can be mapped to every other edge, and if each non-edge can be mapped to every other non-edge.

The definition extends to k-transitive by requiring a similar property for each set of $h \leq k$ vertices: namely, each set of h vertices, which as a subgraph of G induces a graph of a given isomorphism type, is automorphic to every other set of h vertices inducing the same isomorphism type.

The idea of the algorithm is to distinguish a small initial set of vertices (by marking them with the numbers 1,2,.. say). Then we distinguish further vertices as follows: a vertex v will be distinguished if no other vertex is adjacent to the same (already) distinguished vertices as v. The initial set is chosen so that all the vertices can be distinguished eventually, by iterating this process. The initial set of vertices is called a <u>distinguishing set</u>; it is similar to, but not the same as, the distinguishing set of [2].

To test graphs G_1 and G_2 for isomorphism a distinguishing set for G_1 is chosen, of size s say, and all the vertices in G_1 are thereby distinguished. Then we consider every possible distinguishing set of size s for G_2. For each such distinguishing set we obtain a copy of G_2 with all its vertices distinguished. If any of these copies of G_2 is identical to the graph G_1, distinguished as above, then G_1 and G_2 are isomorphic; otherwise they are non-isomorphic. We note that it is necessary to number the vertices in a consistent manner as they are being distinguished. If the size of the distinguishing set is $O(m)$ the algorithm runs in time $O(n^{cm})$, for some constant c. The remainder of the work lies in showing there exist small distinguishing sets.

We just consider graphs that are connected and whose complements are connected. We call such graphs interesting. The only non-interesting strongly regular graphs are unions of equal-sized disjoint cliques and their complements. These can easily be recognized and tested for isomorphism in polynomial time. Henceforth, by a strongly regular graph we intend a graph that is connected and whose complement is connected.

We prove, for $k \geq 4$, that a k-strongly regular graph has a distinguishing set of size $cn^{1/k}\log n + k$, for some constant c, independent of k. Also we prove that all 3-strongly regular graphs, except the <u>layered cliques</u>, have distinguishing sets of size $cn^{1/3}\log n + 3$. The layered cliques are defined in the appendix. They can be recognized and tested for isomorphism in polynomial time. 2-strongly regular graphs, as shown in [2], have distinguishing sets of size $cn^{1/2}\log n + 2$. We deduce there is an isomorphism algorithm for k-strongly regular graphs running in

time $O(n^{cn^{1/k}+k})$, for some constant c independent of k.

Substituting k = logn we deduce that the (logn)-strongly regular graphs have distinguishing sets of size c + logn. These graphs cannot be (c + logn + 1)-transitive since all the vertices are distinguished after marking a set of size c + logn. All graphs which are not (logn)-strongly regular cannot be (logn)-transitive. Thus no interesting graph is (c + logn + 1)-transitive.

3. Size of Distinguishing Sets

Some more definitions are needed. Suppose one vertex v of strongly regular graph G is distinguished. Call v the root, those vertices adjacent to v the level-1 vertices, and those vertices not adjacent to v the level-2 vertices.

Lemma 1:

a) If a strongly regular graph is not connected it is a union of disjoint equal-sized cliques.

b) The complement of a strongly regular graph is a strongly regular graph.

c) If a strongly regular graph and its complement are both connected then it has diameter 2.

Proof: Omitted; see [2]. □

A distinguishing set for a strongly regular graph is also a distinguishing set for its complement. So we can assume the degree of any graph we consider is at most (n-1)/2; if it is not we just look at the complement.

Lemma 2: Let G be an interesting strongly regular graph of degree $d_\emptyset$. G has a distinguishing set of size $O(n/d_\emptyset \log n)$.

Proof: Given in the appendix. □

Lemma 3: Let G be an interesting strongly regular graph. Suppose G is 3-strongly regular. Let v be the root of G. Then no two level-2 vertices are adjacent to exactly the same level-1 vertices.

Proof: Given in the appendix. □

Corollary 1: In a 3-strongly regular graph the root plus the level-1 vertices form a distinguishing set.

Lemma 4: Let G be a (k+1)-strongly regular graph of degree $d_\emptyset$, with $k \geq 2$. Let v be a root of G. If the subgraph induced by the level-1 vertices has a distinguishing set of size $cd_\emptyset^{1/k}\log d_\emptyset + k$, for some constant c, then G has a distinguishing set of size $cd_\emptyset^{1/k}\log d_\emptyset + k+1$.

Proof: Let D_k be a distinguishing set for the subgraph induced by the level-1 vertices of size $cd_\emptyset^{1/k}\log d_\emptyset + k$, for some constant c. Then $D_k \cup \{v\}$ is a distinguishing set for G. □

Lemma 5: If the conditions of lemma 4 hold, G has a distinguishing set of size at most $cn^{1/(k+1)}\log(n) + k+1$, for some constant c.

Proof: If $d_\emptyset \geq n^{1-1/(k+1)}$, using lemma 2, we deduce G has a distinguishing set of size at most $cn^{1/(k+1)}\log n$. Otherwise we note

$$|D_k \cup \{v\}| \leq c(n^{1-1/(k+1)})^{1/k}\log(n) + k+1$$
$$\leq cn^{1/(k+1)}\log(n) + k+1.$$

□

Lemma 5 suggests that by induction we could show a k-strongly regular graph has a distinguishing set of size $O(n^{1/k}\log n) + k$. Unfortunately, we cannot prove the base case: k=2. However, we can prove the result for k=4, and come close enough for k=2 and k=3.

Lemma 6: For graphs with $d_\emptyset \leq (n-1)/2$

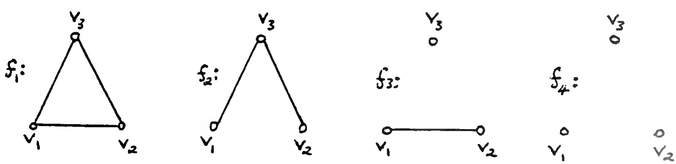
a) The only 2-strongly regular graphs which do not have a distinguishing set of size $O(n^{1/2}\log n)$ are the uninteresting ones.

b) Layered cliques (defined below) are the only interesting 3-strongly regular graphs satisfying both the subgraph induced by their level-1 vertices is uninteresting and $d_\emptyset \leq n^{2/3}/4$.

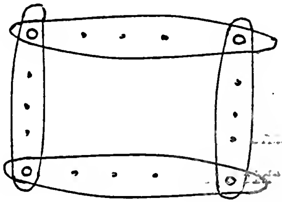
c) Of those 3-strongly regular graphs for which the subgraphs induced by their level-1 vertices are uninteresting only 2 are 4-strongly regular; call these exceptional graphs. For all other interesting 4-strongly regular graphs, the subgraph induced by the level-1 vertices is neither a layered clique, its complement, a 5-cycle, its complement, one of the exceptional graphs, nor one of their complements.

Proof: Given in the appendix. □

To help define a layered clique we first introduce some more notation. For a 3-strongly regular graph we denote the size of the set $A(v_1,v_2,v_3)$ by one of f_1, f_2, f_3, and f_4 according to which subgraph of G is induced by v_1, v_2, and v_3, as illustrated below.



Definition 3: A 3-strongly regular graph is a layered clique if it satisfies $n = k^2$, $d_\emptyset = 2k$, $d_1 = k-1$, $d_2 = 2$, $f_1 = d_1-1$, $f_2 = \emptyset$, and $f_3 = 1$, for some integer k. It is illustrated below.



The graph is a kxk grid; the vertices in each row and in each column form a clique. For a fixed value of k, the layered clique is unique up to isomorphism.

Corollary 2:

a) All 3-strongly regular graphs except the layered cliques have a distinguishing set of size $O(n^{1/3}\log n)$.

b) All k-strongly regular graphs have a distinguishing set of size $O(n^{1/k}\log n) + k$, for $k \geq 4$.

Lemma 7: The two exceptional graphs, layered cliques and uninteresting strongly regular graphs can be recognized and tested for isomorphism in polynomial time. Thus, isomorphism of k-strongly regular graphs can be tested in time $O(n^{cn^{1/k}\log(n)+k})$, for some constant c.

Proof: Follows from the definition of layered cliques. □

4. Conclusions and Further Work.

We have described algorithms running in time $O(n^{n^{1/k}\log n})$. At first sight these seem rather inefficient. But we should remember that strongly regular graphs were thought to be difficult graphs for a general isomorphism algorithm. So the running time should be compared to that for a general graph isomorphism algorithm. The best currently known is $O(d^{n^{1/2}})$, for some constant d [6]. As can be seen, our running time is considerably better than this for large k.

Since no interesting graph is (d + logn)-transitive, for some constant d, we deduce there is a gap between the size of S_n and the size of the automorphism group of an interesting graph.

Open Question: How large is this gap? Can an advantage be obtained to design a faster isomorphism algorithm?

If strongly regular graphs are as hard as was thought it should be possible to find better general isomorphism algorithms. This suggests two possibilities for future work. Either

a) combine the isomorphism algorithms for strongly regular graphs with techniques for general graph isomorphism leading to a faster general graph isomorphism algorithm, or

b) identify further classes of "hard" graphs.

We have not found k-transitive graphs for k>4.

Open Quetion: Find k-transitive graphs or prove they do not exist.

Also, we observe that any k-transitive graph must be k-strongly regular, but not necessarily vice-versa. We have not found any k-

strongly regular graph, either, for k>4.

<u>Open Oestion</u>: Find k-strongly regular graphs or prove they do not exist.

Appendix

We first prove some useful equations which we will use repeatedly. They are:

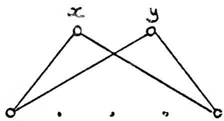
$$d_0(d_0-1) = d_0 d_1 + (n-d_0-1)d_2 \qquad \text{(A)}$$

$$d_1(d_1-1) = d_1 f_1 + (d_0-d_1-1)f_2 \qquad \text{(B)}$$

$$d_0(d_0-1)(d_0-2) = d_0 d_1 f_1 + 3d_0(d_0-d_1-1)f_2 + 3d_0(n-2d_0+d_1)f_3 + (n-d_0-1)(n-2d_0+d_2-2)f_4 \qquad \text{(C)}$$

$$f_3(d_0-d_2) + f_4(n-2d_0-2+d_2) = (n-2d_0-2+d_2)d_2 + (d_0-d_2)(d_1+d_2-d_0+1) \qquad \text{(D)}.$$

We show (A). The edges of the graph are counted in two ways. First we note the graph has $nd_0/2$ edges. Now we count edges out of a pair (x,y) of vertices.



x and y are adjacent to d_1 or d_2 vertices in common. Hence there are $2d_1$ or $2d_2$ edges in the picture above. There are $nd_0/2$ pairs of adjacent (x,y), and $n(n-d_0-1)/2$ pairs of non-adjacent pairs (x,y). So we have counted $nd_0d_1 + n(n-d_0-1)d_2$ edges. Each edge has been counted $2(d_0-1)$ times. To see this consider an edge (v,w); let $A(v) = \{w,v_2,\dots,v_{d_0}\}$, $A(w) = \{v,w_2,\dots,w_{d_0}\}$. (v,w) is counted once for each pair (w,v_i), and once for each pair (v,w_i), for $2 \le i \le d_0$. We deduce (A).

(B) is obtained by considering the strongly regular graph induced by the level-1 vertices. (C) is derived in the same way as (A), except now we consider vertices three at a time. (D) follows by considering the strongly regular graph induced by the level-2 vertices.

Proof of lemma 2: Essentially, this lemma was proven in [2]. We are giving it by way of completeness. First, we need a combinatorial lemma.

Combinatorial lemma: Let S be a set of size n, and let $S_1, S_2, \ldots, S_k$ be subsets of S of size at least p. Then some subset of S of size no greater than O(n logk /p) has a non-empty intersection with each of S_1, $S_2, \ldots, S_k$.

Proof: There are $\binom{n}{i}$ ways to choose an i-tuple from S. Of these at most $\binom{n-p}{i}$ avoid S_1, at most $\binom{n-p}{i}$ avoid S_2, ..., at most $\binom{n-p}{i}$ avoid S_k. Thus the number which avoid some set is at most $k\binom{n-p}{i}$, and if $k\binom{n-p}{i}<\binom{n}{i}$, some i-tuple intersects each set. This is true if

$k < [n/(n-p)]^i$, or $\log k < i \log[n/(n-p)]$, or

$$i > \log k/[\log(n/(n-p))] = \log k/[\log(1/(1-p/n))] = \log k/[\log(\sum_{j=0}^{\infty}(p/n)^j)]$$

which is true if $i \geq \log k/[\log(1+p/n)]$, which is true if $i \geq 2n\log k/p$, since $\log(1+p/n) \geq p/2n$, for $p<n$. □

We show that for each pair of vertices adjacent to a common vertex there are at least $O(d_\emptyset)$ vertices adjacent to one but not the other. Consider the (up to) n^2 posible pairs of vertices, $p_1, p_2, \ldots$. Let S_i be the set of vertices adjacent to exactly one vertex in p_i. Applying the combinatorial lemma, we obtain a set S, of size at most $2n \log(n^2)/[O(d_\emptyset)] = O(n \log n/d_\emptyset)$, satisfying, for each pair (u,v) of vertices adjacent to a common vertex, there exists a vertex $s \in S$ with s

adjacent to exactly one of u and v. Therefore S is a distinguishing set for G. We complete the proof of lemma 2 by proving a sequence of simple lemmas.

Lemma 2.1: Let $d = \min\{d_1, d_2\}$. Then $d_\emptyset^2 \geq nd$.

Proof: From (A) we deduce $d_\emptyset(d_\emptyset - 1) \geq d(n-1)$. That is $d_\emptyset^2 \geq nd$. □

Lemma 2.2: The number of vertices adjacent to exactly one of v or w is at least $d_\emptyset - d$, where v and w are adjacent to a common vertex.

Proof: For vertices v,w,x we have

$$A(v) - A(w) \subset [A(v) - A(x)] \cup [A(x) - A(w)].$$

If v and w are non-adjacent, since the graph is interesting, there is an x with $x \in A(v)$, $x \in A(w)$. Since $|A(v) - A(w)| = d_\emptyset - d_2$, and $|A(v)-A(x)| = |A(x)-A(w)| = d_\emptyset - d_1$, $d_\emptyset - d_2 \leq 2(d_\emptyset - d_1)$.

Similarly we obtain $(d_\emptyset - d_1) \leq 2(d_\emptyset - d_2)$. So $|A(v)| - |A(v) \cap A(w)| \geq \min\{d_\emptyset - d_2, d_\emptyset - d_1\} \geq 1/2 \max\{d_\emptyset - d_1, d_\emptyset - d_2\} = (d_\emptyset - d)/2$.

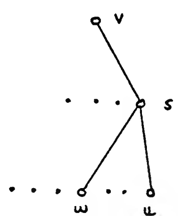
So $|A(v) - A(w)| + |A(w) - A(v)| \geq d_\emptyset - d$. □

Lemma 2.3: $d_\emptyset - d \geq 1/2 d_\emptyset$.

Proof: $dn \leq d_\emptyset^2$, and as $d_\emptyset < n/2$, we have $d < d_\emptyset/2$. □

This completes the proof of lemma 2. □

Proof of lemma 3: Suppose, for a contradiction, that two level-2 vertices (u,w) are adjacent to the same level-1 vertices.



Let v be the distinguished vertex. There are two cases: either u and w are adjacent or they are non-adjacent. But first we consider a special case.

Case Ø: All the level-2 vertices are adjacent to all the level-1 vertices. We prove any such graph must be uninteresting. We have $f_4=d_2=d_\emptyset$; thus we deduce that every pair of level-2 vertices is non-adjacent.

Consider 2 non-adjacent level-1 vertices x and y. Suppose there are r level-2 vertices. Then x and y are adjacent to $d_\emptyset-r-1$ level-1 vertices in common, and hence not adjacent to r-1 of them; let z be one such vertex. Since $f_4=d_2=d_\emptyset$, z is adjacent to the same level-1 vertices as x and y. We deduce the level-1 vertices divide into co-cliques of size r+1, with a pair of co-cliques forming a complete bipartite graph. But then G is just the complement of a union of equal-sized disjoint cliques.

Case 1: u and w are adjacent. We prove that all graphs of this form are covered by case Ø. Since A(u,v) = A(u,v,w), $d_2=f_3$. Suppose u is also adjacent to level-2 vertex x; then A(u,v,x) = f_3 = d_2, so x is adjacent to the same level-1 vertices as u (and w). If w and x are not adjacent we obtain case Ø; if we do not have case Ø then the level-2 vertices form disjoint cliques, the vertices in each clique being adjacent to the same level-1 vertices. The cliques are of the same size: $d_\emptyset-d_2+1$.

Let s be a level-1 vertex adjacent to u. $|A(u,s)| = d_1$. s is also adjacent to u and v so $d_\emptyset = |A(s)| \geq d_1+2$. Now u is adjacent to A(u,w) $\cup$ {w}, thus $d_\emptyset = d_1+1$. Contradiction; so case Ø must hold. □

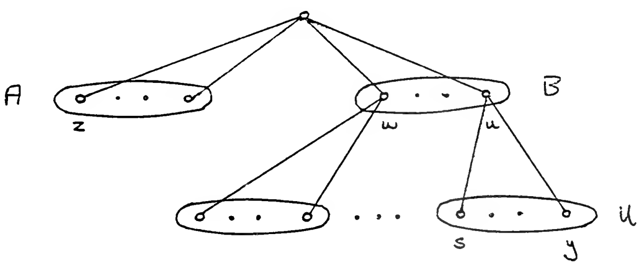
Case 2: u and w are not adjacent. Again, we show that all such graphs are covered by case Ø. Since $A(u,v) = A(u,v,w)$, $d_2=f_4$. Suppose u is also non-adjacent to level-2 vertex x; then $|A(u,v,x)| = f_4 = d_2$, so x is adjacent to the same level-1 vertices as u (and w). If x is adjacent to w we obtain case Ø; if case Ø does not apply the vertices form co-cliques, with the vertices in each co-clique being connected to the same level-1 vertices. Each pair of co-cliques forms a complete bipartite graph. We show there is exactly one coclique, giving case Ø. Since $|A(u,v)| = |A(u,w)| = |A(u,v,w)|$, u and w are adjacent to no level-2 vertices in common, and hence there is just one co-clique.

Proof of lemma 6:

Part (a) follows from lemmas 1 and 2 since an interesting graph has diameter 2, and so satisfies $d_{\emptyset}>n^{1/2}$.

The proof of part (b) falls into two cases: the level-1 vertices are either the union of equal-sized disjoint cliques or are the complement thereof.

Case b.1.1: The level-1 vertices form 2 cliques. The case with the cliques having size 1 is handled in b.2.



Let v be the distinguished vertex, and let A and B be the cliques adjacent to v. Let u be a vertex in B. We show that u is adjacent to a clique U of d_1+1 level-2 vertices; further if w is a level-1 vertex adjacent to u, w is adjacent to none of the vertices in U. Thus any level-2 vertex is adjacent to at most one vertex in B. Since $|A(u,v)| = |A(u,w)|$, and as w and u are adjacent to the other vertices in B and to v, w and u are adjacent to no level-2 vertices in common. So any vertex in U is adjacent to just one vertex in B. By considering B we observe $f_1=d_1-1$, and thus the d_1+1 level-2 vertices adjacent to u form a clique.

We show $d_2=2$. Since any level-2 vertex is adjacent to at most one vertex in B, by symmetry any level-2 vertex is adjacent to at most one vertex in A. That is $d_2 \leq 2$. As the graph is connected and not complete we have $d_2=1$ or $d_2=2$.

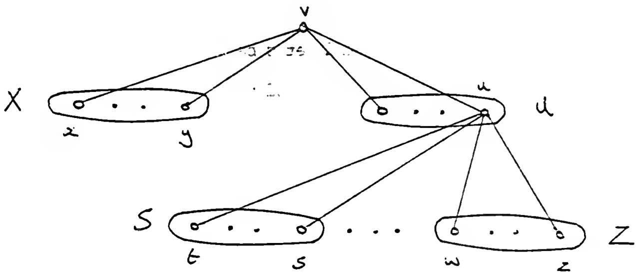
Let s and y be two vertices in U and let z be a vertex in A. We show $d_2 \geq 2$. $f_3 = |A(v,y,s)| \geq 1$. Suppose y and z are not adjacent; then $f_3 = |A(v,z,y)|$. Thus y is adjacent to a vertex in A, and so $d_2 \geq 2$. We deduce $d_2=2$.

We complete the description of the graph. By symmetry each vertex in A must be adjacent to a clique of level-2 vertices of size d_1+1. Let z be a vertex in A. Since $|A(z,u)| = d_2 = 2$, z and u are adjacent to exactly one level-2 vertex in common. Likewise for each pair of vertices, one taken from A, and one taken from B. There are d_1+1 cliques adjacent to vertices in B, so each vertex z in A is adjacent to one vertex in each of these cliques, and these vertices form the clique to which z is adjacent. It is straightforward to check that the graph just described satisfies $d_\emptyset = 2d_1+2$, $d_2 = 2$, $f_2 = \emptyset$, $f_1 = d_1-1$, and $f_3 = 1$,

so the graph can have no other edges. A little thought shows that up to isomorphism, for a given n, there is at most one such strongly regular graph, which we call a layered clique.

$d_1=1$ gives a 4-strongly regular graph: one of the excetional graphs mentioned in part (c). For $d_1 \geq 2$, we show the graphs are not 4-strongly regular. For, choosing $z \in A$, not adjacent to either s or $y (\in U)$, we observe $|A(v,z,s,y)| = \emptyset$; but $|A(v,w,s,y)| = 1$, and the two sets of vertices induce the same subgraph; hence the graph is not 4-strongly regular.

Case b.1.2: The level-1 vertices form $r>2$ cliques. We need only consider the case of cliques having size at least 2, for the case with cliques of size 1 is handled below, in case b.2.



Let v be the distinguished vertex. We argue that each level-1 vertex is adjacent to r-1 cliques of d_1+1 vertices each. Let u be a level-1 vertex in clique U; it is adjacent to $(r-1)(d_1+1)$ level-2 vertices since $d_\emptyset = r(d_1+1)$. As argued above, any level-2 vertex is adjacent to just one vertex in U. And as $f_1 = d_1-1$ the vertices adjacent to u must divide into cliques of d_1+1 vertices each.

We show $d_2 \geq r$. Consider two adjacent level-2 vertices w and z, in clique Z, both adjacent to u. Let x, in clique X, be a level-1 vertex not adjacent to u. $A(v,z,w) = f_3 \geq 1$; if w is not adjacent to x, $|A(v,x,w)| = f_3 \geq 1$; so there is some level-1 vertex y adjacent to both x and w. Thus there is at least one vertex in X adjacent to w. But this is true for each level-1 clique, so $d_2 \geq r$.

Now, we show $d_2 = r$. We note $f_2 = \emptyset$. Consider A(y,u,w), where y in X is adjacent to w, but not to u. Since $f_2 = |A(y,u,w)| = \emptyset$, we deduce y is adjacent to no other vertices in the clique in which w lies. Hence y is adjacent to at most one vertex in each of the r-1 level-2 cliques to which u is adjacent. so $d_2 = |A(u,y)| \leq r$. Hence $d_2 = r$.

We also show $f_3 = 1$. Consider A(v,y,w) where w is adjacent to y. $|A(v,y,w)| = f_2 = \emptyset$, so w is adjacent to no other vertices in X. Let x be another vertex in X. $f_3 = |A(v,x,w)| = |\{y\}| = 1$.

Now, we obtain the equation $(f_4-1)(d_1+1) = (d_2-1)$. As argued above, z is adjacent to one vertex in each level-1 clique. Let S be a level-2 clique adjacent to u, distinct from Z, and let s and t be two vertices in S. $|A(z,s,v)| = f_4$, so z and s are adjacent to a vertex in each of f_4-1 level-1 cliques besides U. Likewise for z and t. A(v,s,t) = {u} as $|A(v,s,t)| = f_3 = 1$; so z and t are adjacent to vertices in cliques distinct from those having vertices to which both z and s are adjacent. As there are d_1+1 vertices in S, we have accounted for $(f_4-1)(d_1+1)$ level-1 cliques, besides U. We argue there are no others.

Let m be a level-1 vertex adjacent to z but non-adjacent to all the vertices in S, if there is such. $|A(m,t,v)| = f_3 = 1$, for all $t \in S$, so each t is adjacent to a vertex in M, the clique containing m. Since s

and t are adjacent to no vertices in common in M, we deduce $|M| > |S|$. Contradiction. Hence $(f_4-1)(d_1+1) = d_2-1$.

We count the vertices in the graph. Remembering that every level-2 vertex is adjacent to a vertex in U we obtain

$$n = 1 + d_\emptyset + (d_1+1)(d_2-1)(d_1+1)$$
$$= 1 + d_\emptyset + d_\emptyset(d_1+1) - (d_1+1)^2.$$

We know $d_\emptyset(d_\emptyset-1) = d_\emptyset d_1 + (n-d_\emptyset-1)d_2$, $f_2=\emptyset$, $f_3=1$, $f_1 = d_1-1$, $d_\emptyset = d_2(d_1+1)$.

On substituting in (D) we obtain:

$d_2 = (d_1+1)^2+1$; so $f_4=d_1+2$, $n=(d_1+2)[(d_1+1)^3+1]$, and $d_\emptyset=(d_1+1)[(d_1+1)^2+1]$.

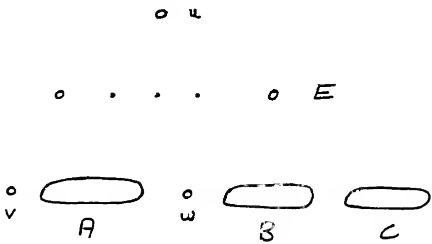
$d_1=1$ gives us a 4-strongly regular graph: one of the exceptional graphs mentioned in part (c). For $d_1\geq 2$, we show the graphs are not 4-strongly regular. Choose $x\in X$, not adjacent to either w or z ($\in Z$). Then $|A(v,x,w,z)| = \emptyset$. Choose $r\neq u$ from U; then $|A(v,r,w,z)| = 1$. The two sets of vertices induce the same subgraph; hence the graph is not 4-strongly regular. Also, for $d_1\geq 2$, $d_\emptyset\geq n^{2/3}/4$.

<u>Case b.2</u>: The subgraph induced by the level-1 vertices is the complement of a union of equal-sized disjoint cliques.

<u>Case b.2.1</u>: The subgraph is totally disconnected. We prove all such interesting graphs satisfy $d_\emptyset\geq n^{2/3}/2$. Further, we prove none of these graphs are 4-strongly regular, except for the 5-cycle.

From (A) we obtain $d_\emptyset(d_\emptyset-1)=d_2(n-d_\emptyset-1)$, and from (C) we know $d_\emptyset(d_\emptyset-1)(d_\emptyset-2) = f_4(n-d_\emptyset-1)(n-2d_\emptyset-2+d_2)$. If $d_\emptyset=2$ we obtain the 5-cycle (the 4-cycle is not an interesting graph). For $d_\emptyset>2$ we have $f_4\geq 1$.

If $n>3d_0$, from (C) we deduce $d_0^3>2n^2/9$, so $d_0 \geq n^{2/3}/2$. And for $d_0 \geq 2$, $n \leq 3d_0$ implies $d_0 \geq n^{2/3}/2$.



Suppose one of these graphs is 4-strongly regular. Let u be the distinguished vertex, E the set of level-1 vertices, and v a level-2 vertex. Let A be the set of level-2 vertices adjacent to v, let w be another level-2 vertex not adjacent to v, let B be the set of level-2 vertices adjacent to w but not to v, and let C be the set of all the other level-2 vertices. Then $|A| = d_0-d_2$, $|B| = d_0-2d_2+f_4$, $|C| = n-3d_0-3+3d_2-f_4$. We count the edges between the vertices in C and E in two ways. There are d_2 edges from each vertex in C to a vertex in E; that is $d_2(n-3d_0-3+3d_2-f_4)$ edges. There are f_4 vertices in E adjacent to both v and w; each such vertex is adjacent to d_0-1 vertices in C. There are $2(d_2-f_4)$ vertices in E adjacent to exactly one of v and w; each such vertex is adjacent to d_0-1-d_2 vertices in C. And there are $d_0-2d_2+f_4$ vertices in E adjacent to neither v nor w; each such vertex is adjacent to $d_0-1-2d_2+f_4$ vertices in C. We deduce

$$d_2(n-3d_0-3+3d_2-f_4) = f_4(d_0-1) + 2(d_2-f_4)(d_0-1-d_2) + (d_0-2d_2+f_4)(d_0-1-2d_2+f_4).$$

That is, $d_2(n-d_\emptyset+d_2-3) = f_4(d_\emptyset-d_2+f_4) + d_\emptyset(d_\emptyset-1)$, or

$$d_2(d_2-2) = f_4(d_\emptyset-d_2+f_4).$$

From (A) and (C) we deduce

$f_4[d_\emptyset(d_\emptyset-1)-(d_2(d_\emptyset-d_2+1)] = d_2^2(d_\emptyset-2)$, and on substituting, we obtain

$$\begin{aligned} \emptyset &= d_2^4(d_\emptyset-d_2) \\ &\quad +(2d_\emptyset^4-5d_\emptyset^3d_2+10d_\emptyset^2d_2^2-11d_\emptyset d_2^3+6d_2^4) \\ &\quad -(4d_\emptyset^3-d_\emptyset^2d_2+2d_\emptyset d_2^2+3d_2^3) \\ &\quad +2(d_\emptyset+d_2)^2. \end{aligned}$$

As shown in the proof of lemma 2, $2(d_\emptyset-d_2)\geq(d_\emptyset-d_1)=d_\emptyset$, so $d_2\leq d_\emptyset/2$. Careful checking shows $d_\emptyset=2$, $d_2=1$ is the only solution. Thus, except for the 5-cycle, none of these graphs is 4-strongly regular.

Case b.2.2: The subgraph induced by the level-1 vertices is the complement of a union of r>1 equal-sized disjoint cliques.

We assume there are at least two vertices in each coclique. For if not, the level-1 vertices form a single clique, which gives a graph consisting of a single clique. We have $d_1=d_\emptyset(r-1)/r$ and $d_2\geq d_1+1$. From (A) we obtain: $d_\emptyset^2 \geq (n-1)[d_\emptyset(r-1)/r + 1]$, so $d_\emptyset > (n-1)[(r-1)/r]$. As $r\geq 2$, $d_\emptyset>(n-1)/2$. Thus this type of graph can be dealt with by looking at its complement.

We now prove part (c).

The only cases we need consider are those in which the level-1 vertices either form a layered clique, form the complement of a layered

clique, form a five cycle, form the complement of a five cycle, form one of the exceptional graphs, or form the complement of one of the exceptional graphs. We show none of these occurs.

<u>Case c.1</u>: The subgraph induced by the level-1 vertices is the complement of a layered clique.

Suppose that in the layered clique there are r vertices in each clique. Then in the graph we are considering $d_1=r^2$, $d_\emptyset=r(r+2)+1$, and $d_2\geq r(r-1)+1$. We show $d_\emptyset>(n-1)/2$, and so this type of graph can be dealt with by looking at its complement.

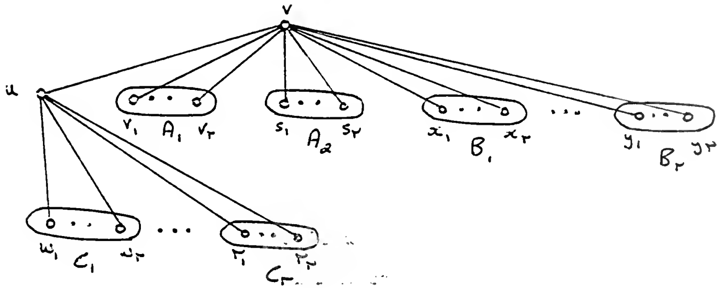
We count the level-2 vertices. From each level-1 vertex there are $2r$ edges to level-2 vertices, and from each level-2 vertex there are d_2 edges to level-1 vertices, giving us $2rd_\emptyset/d_2$ level-2 vertices.

If $d_\emptyset\leq(n-1)/2$, there are at least $d_\emptyset$ level-2 vertices, so $2r\geq r(r-1)+1$. The only solutions are $r=1$ and $r=2$. On trying to draw the graph for $r=1$ we discover it is the layered clique on 9 vertices, a graph we already know about. For $r=2$ we find the level-1 vertices form a layered clique, a case handled below.

<u>Case c.2</u>: The subgraph induced by the level-1 vertices is a layered clique.

Let r denote the number of vertices in a level-1 clique. The case $r=1$ gives us $d_\emptyset=4$, $d_1=2$, and $d_2\geq 3$; so $d_2=3$ or $d_2=4$. We have from (A), either $4=3(n-5)$ or $4=4(n-5)$, implying $d_2=4$ and $n=6$. But this is just the complement of a union of three 2-cliques, an uninteresting graph. So $r>1$.

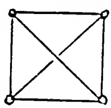
We show, for graphs with $r>1$, that $d_\emptyset>(n-1)/2$.



Let the distinguished vertex be v, and suppose the level-1 vertices have u as their distinguished vertex, A_1 and A_2 being the cliques adjacent to u, and B_1, B_2, ..., B_r being the cliques adjacent to vertices in A_1.

u must be adjacent to r^2 level-2 vertices. Since $d_1=2r$ and $f_1=r-1$ we deduce that each vertex in A_1 is adjacent to r level-2 vertices that are also adjacent to u. Let the r vertices adjacent to $v_i \in A_i$ form C_i. We argue C_i is a clique. First, some more notation.

g_1:

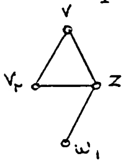


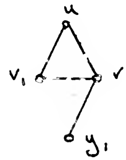
Since $g_1=f_1-1$, the vertices in C_i form a clique (remember, this graph is 4-strongly regular). Let us indicate 2 vertices in each clique.

Consider a vertex $s_i \in A_2$. We show s_i is adjacent to one vertex in each C_j. $2 = |A(v,u,x_1)| = f_2$. As $|A(v_1,s_i,u)| = f_2$, we deduce s_i is adjacent to exactly one vertex in C_1. Now we show s_i and s_j, $i \neq j$, are

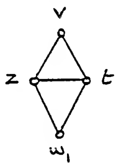
adjacent to distinct vertices in C_k. For $f_1 = |A(v,v_1,v_r)| = r-1$; and $f_1 = |A(u,s_i,s_j)|$; so s_i, s_j, and u have no level-2 vertices in common. WLOG let s_i be adjacent to w_i and r_i, for $i=1,2,\ldots,r$.

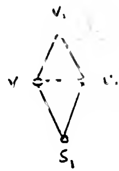
We show $f_3=4$. As $\{u,w_r\} \subset A(v,v_r,w_1)$, any other vertex in this set lies in B_r. Suppose there is one vertex $z \in B_r$, adjacent to w_1. Then $|A(w_1,z,v_r,v)| = |A(v,u,v_1,y_1)| = 1$.





Implying there is a second vertex $t \in B_r$, adjacent to w_1. Also $|A(v,w_1,z,t)| = |A(u,v,v_1,s_1)| = \emptyset$.





Thus w_1 is adjacent to zero or two vertices in B_r. That is $f_3=2$ or $f_3=4$.

If $f_3=2$, in the set $B_1 \cup B_2 \cup \ldots \cup B_r$, w_1 is adjacent to at most one vertex, namely the vertex x_1 adjacent to both v_1 and s_1. But then $f_3 = |A(v,y_r,w_1)| = \emptyset$, where y_r is chosen to be non-adjacent to both x_1 and s_1. Contradiction. So $f_3=4$.

Now, we show $d_2=2(r+1)$. Since $f_3=4$, w_1 is adjacent to 2 vertices in each of $B_2, B_3, \ldots, B_r$. Since $2 = f_2 = |A(v,v_1,w_1)|$, w_1 is adjacent to exactly one vertex in B_1. $d_2 = |A(v,w_1)|$. So $d_2 = 2(r-1)+4 =$

$2(r+1)$.

Substituting into (A) we deduce

$$n = r^3/2 + 3r^2/2 + 2r + 2.$$

Substituting into (D) we obtain:

$$f_4 = 4(r+1)(r-1)/r^2,$$

which implies $r=2$ and $f_4=3$. So $n=16$ and $d_\emptyset=9$. Since $d_\emptyset>(n-1)/2$ we deal with this type of graph by looking at its complement.

Case c.3: The subgraph induced by the level-1 vertices is a 5-cycle (or the complement of a 5-cycle; it is a 5-cycle too).

$d_\emptyset=5$, $d_1=2$; substituting into (A) we obtain $d_2(n-6)=10$. Either $d_2=1$ and $n=16$, or $d_2=2$ and $n=11$, or $d_2=5$ and $n=8$.

We also have $f_1=\emptyset$. Substituting into (B) we obtain $2 = 2f_2$; so $f_2=1$. Now $d_2>f_2$; so $d_2=2$ or $d_2=5$. Substituting into (C) and (D) we find neither of these cases holds.

Case c.4: The subgraph induced by the level-1 vertices is an exceptional graph or its complement.

We have already dealt with the exceptional graph that is a layered clique in cases c.1 and c.2. So we have only to consider the exceptional graph of case b.1.2, or its complement, being the graph induced by the level-1 vertices.

First, the case with the level-1 vertices inducing the exceptional graph. $d_\emptyset=27$, $d_1=10$, $d_2\geq 6$, $f_1=1$, and $f_2=5$. From $d_\emptyset(d_\emptyset-d_1-1)=d_2(n-d_\emptyset-1)$, and remembering the assumption $d_\emptyset\leq(n-1)/2$ we

deduce $d_2=6$, 8,9, 12, or 16 and n=100, 82, 76, 64, or 55, respectively. On substituting into (C) and (D) we discover none of these possibilities hold, except for $d_2=12$; but this graph is not 4-strongly regular.

Likewise, for the case with the level-1 vertices inducing the complement of the exceptional graph, $d_0=27$, $d_1=16$, $d_2\geq 9$, $f_1=10$, and $f_2=8$. We deduce $d_2=9$, or 10, and n=58, or 55, respectively. Again, on substituting into (C) and (D) we find neither of these possibilities holds.
□

Acknowledgements

This work was started as a result of conversations with Bengt Aspvall. I also had several instructive conversations with Neil Immerman. I am indebted to both.

References

[1] B. Aspvall, private communication.

[2] L. Babai, On the complexity of canonical labelling of strongly regular graphs, SIAM J. Comput., Vol. 9, No. 1, Jan. 1980.

[3] Corneil and Gotlieb, An efficient algorithm for graph isomorphism, JACM, Vol. 17, Jan. 1970.

[4] Cvetkovic, Doob, and Sachs, Spectra of graphs, Academic Press, 1980.

[5] Z. Galil, C.Hoffmann, E.Luks, C. Schnorr, A. Weber, An $O(n^3 \log n)$ deterministic and an $O(n^3)$ probabilistic isomorphism test for trivalent graphs, Proc. 23rd Annl. FOCS, 1982, pp. 126,133.

[6] E. Luks, communicated by Z. Galil.

[7] E. Luks, Isomorphism of graphs of bounded valence can be tested in polynomial time, Proc. 21st Annl. FOCS, 1980, pp. 42-49.

[8] G. Miller, On the $n^{\log n}$ isomorphism technique, Proc. 10th Annl. SIGACT Conf., 1978.